Karakteri konačnih Abelovih grupa

Klarić, Matija

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Matija Klarić

Karakteri konačnih Abelovih grupa

Završni rad

Osijek, 2015.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Matija Klarić

Karakteri konačnih Abelovih grupa

Završni rad

Mentor: doc. dr. sc. Ivan Matić

Osijek, 2015.

Sažetak

U ovom radu proučavat ćemo konačne Abelove grupe i posebnu vrstu aritmetičkih funkcija, takozvane Dirichletove karaktere. Dirichletovi karakteri mogu se proučavati i bez poznavanja elementarne teorije grupa, no već minimalna količina ove teorije pojednostavit će raspravu i smjestiti ih u prirodnije okruženje. Poznavanje Dirichletovih karaktera nužno je za razumijevanje Dirichletovog teorema o prostim brojevima u aritmetičkim nizovima.

Ključne riječi

grupa, Abelova grupa, konačna grupa, red grupe, podgrupa, karakteri, ortogonalnost, reducirani sustav ostataka, Dirichletovi karakteri

Abstract

This paper studies finite Abelian groups and certain arithmetical functions called Dirichlet characters. Although the study of Dirichlet characters can be undertaken without any knowledge of groups, the introduction of a minimal amount of group theory places the theory of Dirichlet characters in a more natural setting and simplifies some of the discussion. The knowledge of Dirichlet characters is required for discussion on Dirichlet's theorem on primes in arithmetical progressions.

Key words

group, Abelian group, finite group, group order, subgroup, characters, orthogonality, reduced residue system, Dirichlet characters

Sadržaj

Poglavlje 1

Uvod

Karakterima konačnih Abelovih grupa bavit ćemo se nakon što uvedemo osnovne pojmove teorije grupa, iskažemo i dokažemo najvažnije teoreme i damo par primjera koji će nam koristiti kasnije. Karakteri konačnih Abelovih grupa posebna su preslikavanja sa konačne Abelove grupe G u polje kompleksnih brojeva. Pokazuje se da karaktera konačne grupe G ima točno onoliko koliko je njezin red te da zadovoljavaju zanimljive relacije ortogonalnosti.

Ovakva preslikavanja prvi su puta proučavana u teoriji brojeva. Johann Peter Gustav Lejeune Dirichlet je pomoću karaktera grupe $\mathbb{Z}_{/(m)}$ dokazao da za $(a, m) = 1$ postoji beskonačno mnogo prostih brojeva p kongruentnih a modulo m. Ako je specijalno G reducirani sustav ostataka modulo fiksni prirodni broj k, karaktere te grupe njemu u čast nazivamo Dirichletovima.

Dirichlet je pomoću karaktera konačnih Abelovih grupa definirao i L-redove, koji su prirodno proširenje Riemannove zeta-funkcije. Iz Dirichletovih L-redova su se kasnije razvile L-funkcije, danas temeljni pojam analitičke teorije brojeva. Dirichletove pojmove prvi je proširio Riemann, do analitičkih funkcija koje se pojavljuju u brojnim istaknutim problemima u algebri i teoriji brojeva, poput Generalizirane Riemannove hipoteze.

Poglavlje 2

Elementarna teorija grupa

1. Definicije

Definicija 2.1. *Uređen par nepraznog skupa G i binarne operacije $\cdot$ nazivamo grupom ukoliko vrijedi iduće:*

- *Zatvorenost:* $\forall a, b \in G, \quad a \cdot b \in G$
- *Asocijativnost:* $\forall a, b, c \in G, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- *Postojanje neutralnog elementa:* $\exists e \in G \;\text{ t.d. }\; \forall a \in G, \quad a \cdot e = e \cdot a$
- *Postojanje inverza:* $\forall a \in G \;\; \exists b \in G \;\text{ t.d. }\; a \cdot b = b \cdot a = e.$

Napomena 2.1. *U daljnjem tekstu ćemo umjesto $a \cdot b$ pisati samo ab, a umjesto o uređenom paru $(G, \cdot)$ govorit ćemo samo o grupi G. Neutralni element grupe je jedinstven, kao i inverz svakog elementa. Inverz elementa a označavamo s a^{-1}.*

Definicija 2.2. *Grupu G nazivamo Abelovom (komutativnom) ako $\forall a, b \in G, ab = ba$.*

Definicija 2.3. *Grupu G nazivamo konačnom ako je G konačan skup. U tom slučaju broj elemenata skupa G zovemo redom grupe G i označavamo s $|G|$. U suprotnom grupu nazivamo beskonačnom.*

Definicija 2.4. *Neprazan podskup H grupe G koji je i sam grupa (uz istu operaciju) nazivamo podgrupom grupe G. Označavamo s $H \leq G$.*

2. Primjeri

Primjer 2.1. *Skup cijelih brojeva* $\mathbb{Z}$ *uz operaciju zbrajanja je beskonačna Abelova grupa. Neutralni element u toj grupi je* 0*, a inverz cijelog broja* n *je* $-n$*.*

Primjer 2.2. *Svaka grupa* G *ima barem dvije podgrupe: samu sebe i skup koji sadrži samo neutralni element,* $\{e\}$*. Ove podgrupe zovemo trivijalnima.*

Primjer 2.3. *Skup* $\mathbb{C}\backslash\{0\}$ *je beskonačna Abelova grupa uz uobičajeno množenje kompleksnih brojeva. Neutralni element ovdje je* 1*. Inverz elementa* z *je njemu recipročan element* $\frac{1}{z}$*. Jedna podgrupa ove grupe je skup svih kompleksnih brojeva modula* 1*.*

Primjer 2.4. *Primjer konačne grupe je skup* $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ *uz uobičajeno množenje kompleksnih brojeva, gdje je* $\alpha = e^{\frac{2\pi i}{n}}$*. Ovu grupu reda* n *nazivamo grupom* n*-tih korijena jedinice. Uočimo da je ovo podgrupa obiju grupa iz prethodnog primjera.*

3. Elementarna svojstva grupa

Neka je za potrebe idućih teorema G proizvoljna grupa. Ukoliko nije posebno naglašeno, G ne smatramo Abelovom niti konačnom.

Teorem 2.1. *Ukoliko elementi* $a, b, c \in G$ *zadovoljavaju neki od identiteta:*

$$ac = bc \qquad \textit{ili} \qquad ca = cb,$$

tada je $a = b$*.*

Dokaz: U prvom slučaju pomnožimo svaku stranu jednakosti zdesna, a u drugom slijeva s c^{-1} te iskoristimo asocijativnost.

Teorem 2.2. *U grupi* G *vrijedi:*

- $e^{-1} = e$
- $\forall a \in G, \quad (a^{-1})^{-1} = a$
- $\forall a, b \in G, \quad (ab)^{-1} = b^{-1}a^{-1}$
- $\forall a, b \in G$ *jednadžba* $ax = b$ *ima jedinstveno rješenje* $x = a^{-1}b$*, a jednadžba* $ya = b$ *ima jedinstveno rješenje* $y = ba^{-1}$*.*

Dokaz: Dokažimo posljednju točku. Zbog asocijativnosti u G imamo:

$$a(a^{-1}b) = (aa^{-1})b = b \quad i \quad (ba^{-1})a = b(a^{-1}a) = b.$$

Rješenja jednadžbi su jedinstvena zbog zakona kraćenja iz prethodnog teorema.

Definicija 2.5. *Za $a \in G$ i proizvoljan cijeli broj n definiramo a^n sljedećim relacijama:*

$$a^0 = e, \qquad a^n = aa^{n-1}, \qquad a^{-n} = (a^{-1})^n, \quad n > 0.$$

Sljedeća se svojstva potenciranja lako dokažu indukcijom, pa izostavljamo dokaz.

Teorem 2.3. *Za proizvoljan $a \in G$ te proizvoljne cijele brojeve m i n vrijedi:*

$$a^m a^n = a^{m+n} = a^n a^m \qquad i \qquad (a^m)^n = a^{mn} = (a^n)^m.$$

Nadalje, ako $a, b \in G$ komutiraju, vrijedi:

$$a^n b^n = (ab)^n.$$

Teorem 2.4. *Neprazan podskup H grupe G je podgrupa grupe G ako i samo ako vrijede sljedeća dva svojstva:*

- *Zatvorenost:* $\forall a, b \in H, \quad ab \in H$
- *Postojanje inverza:* $\forall a \in H, \quad a^{-1} \in H.$

Dokaz: Jasno je da svaka podgrupa H grupe G zadovoljava oba gornja svojstva. Obratno, neka neprazan podskup H grupe G zadovoljava ova svojstva. Asocijativnost vrijedi u H jer vrijedi u čitavoj grupi G. Kako je H neprazan skup, postoji neki element $a \in H$. Zbog drugog svojstva je i $a^{-1} \in H$. Sada je zbog prvog svojstva $aa^{-1} = e \in H$. Dakle, H je grupa, tj. podgrupa grupe G.

4. Konstrukcija podgrupa

Jedan od načina konstrukcije neke podgrupe grupe G jest da odaberemo proizvoljni element $a \in G$ te načinimo skup svih njegovih potencija a^n, $n = 0, \pm 1, \pm 2, ...$ Ovaj skup je podgrupa grupe G jer očito zadovoljava oba svojstva iz prethodnog teorema. Taj skup nazivamo cikličkom grupom generiranom elementom a te označavamo s $\langle a \rangle$. Nadalje, uočimo da je $\langle a \rangle$ uvijek Abelova grupa, čak i kada G nije.

Ukoliko je $a^n = e$ za neki pozitivan cijeli broj n, postojat će i najmanji $n > 0$ s ovim svojstvom. Tada će podgrupa $\langle a \rangle$ biti konačna grupa reda n.

$$\langle a \rangle = \{a, a^2, \dots, a^{n-1}, a^n = e\}.$$

Takav n zovemo redom elementa a.
Ranije spomenuta grupa n-tih korijena jedinice je primjer cikličke grupe reda n.
Idući teorem govori da je svaki element konačne grupe konačnog reda.

Teorem 2.5. *Neka je G konačna te $a \in G$. Tada postoji pozitivan cijeli broj $n \leq |G|$ takav da je $a^n = e$.*

Dokaz: Označimo $|G| = g$. Tada barem dva od idućih $g+1$ elemenata u G moraju biti jednaki:

$$e, a, a^2, \dots, a^g.$$

Pretpostavimo da je $a^r = a^s$, gdje je $0 \leq s < r \leq g$. Sada imamo:

$$e = a^r (a^s)^{-1} = a^{r-s}$$

pa je dovoljno uzeti $n = r - s$.

Znamo da svaka grupa G ima dvije trivijalne podgrupe: $\{e\}$ i G. Za konačnu Abelovu grupu G postoji jednostavan postupak konstrukcije rastućeg niza podgrupa između $\{e\}$ i G. Opisat ćemo ga nešto kasnije, a temelji se sljedećem: ako je H podgrupa konačne grupe G te a proizvoljan element iz G, sigurno postoji $n \in \mathbb{N}$ takav da je $a^n \in H$. Ako je sam a sadržan u H, jednostavno uzmemo $n = 1$. Ako $a \notin H$, možemo za n uzeti red elementa a, s obzirom da je $a^n = e \in H$. No, moguće je da postoji i manja potencija od a u H. Po principu dobrog uređenja, postoji najmanji $n \in \mathbb{N}$ takav da je $a^n \in H$. Takav n zovemo indikatorom od a u H.

Teorem 2.6. *Neka je H podgrupa konačne Abelove grupe G, $H \neq G$. Neka je $a \in G$ proizvoljan, $a \notin H$, te l indikator od a u H. Tada je skup produkata*

$$M = \{xa^k : x \in H, k = 0, 1, 2, \dots, l-1\}$$

podgrupa grupe G koja sadrži H. Štoviše, za red grupe M vrijedi

$$|M| = l|H|.$$

Dokaz: Da bismo pokazali da je $M \leq G$, pokažimo prvo da vrijedi zatvorenost. Odaberimo dva elementa u M, xa^k i ya^j, gdje su $x, y \in H$ te $0 \leq k < l, 0 \leq j < l$. Kako je G Abelova, produkt ovih elemenata je

$$xa^k ya^j = (xy)a^k a^j = (xy)a^{k+j}.$$

Neka je sada $k + j = ql + r$, gdje je $0 \leq r < l$. Imamo

$$a^{k+j} = a^{ql+r} = a^{q^l} a^r = za^r,$$

gdje je $z = a^{q^l} = (a^l)^q \in H$. Zato je

$$(xy)a^{k+j} = (xyz)a^r = wa^r,$$

gdje je $w \in H$ i $0 \leq r < l$. Ovime smo pokazali zatvorenost. Preostaje pokazati da se inverz svakog elementa iz M također nalazi u M. Odaberimo proizvoljan $xa^k \in M$. Ako je $k = 0$, tada je inverz x^{-1} i on je u M. Ako je pak $0 < k < l$, inverz je element ya^{l-k}, gdje je $y = x^{-1}(a^k)^{-1}$ te je i on u M. Ovime smo pokazali da je $M \leq G$, a očito je da M sadrži H. Zanima nas još red grupe M. Označimo $|H| = h$. Za $x \in H$ te $k = 0, 1, 2, \ldots, l-1$, dobivamo hl produkata xa^k. Ako pokažemo da su svi ovi produkti različiti, slijedit će $|M| = hl$. Pretpostavimo suprotno, tj. neka je

$$xa^k = ya^j, \quad 0 \leq j \leq k < l.$$

Tada je $a^{k-j} = x^{-1}y$ i $0 \leq k - j < l$. Kako je $x^{-1}y \in H$, mora biti $a^{k-j} \in H$, pa je nužno $k = j$ i odatle $x = y$.

Poglavlje 3

Karakteri konačnih Abelovih grupa

Definicija 3.1. *Neka je G proizvoljna grupa. Kompleksnu funkciju f definiranu na G nazivamo karakter grupe G ako f ima svojstvo multiplikativnosti*

$$f(ab) = f(a)f(b), \quad \forall a, b \in G$$

i ako je $f(c) \neq 0$ za neki $c \in G$.

Teorem 3.1. *Ako je f karakter konačne grupe G te e neutralni element u G, vrijedi $f(e) = 1$ i svaka vrijednost $f(a), a \in G$ je korijen jedinice. Drugim riječima, ako je $a^n = e$, onda je $f(a)^n = 1$.*

Dokaz: Uzmimo $c \in G$ takav da je $f(c) \neq 0$. Kako je $ce = c$, imamo

$$f(c)f(e) = f(ce) = f(c),$$

pa je očito $f(e) = 1$. Ako je $a^n = e$, onda imamo $f(a)^n = f(a^n) = f(e) = 1$.

Primjer 3.1. *Svaka grupa G ima barem jedan karakter, funkciju koja je identički jednaka 1. Ovaj karakter nazivamo glavni. Idući teorem govori da ih za Abelovu grupu konačnog reda većeg od 1 postoji još.*

Teorem 3.2. *Neka je G konačna Abelova grupa reda n. Tada postoji točno n različitih karaktera grupe G.*

Dokaz: Ranije smo pokazali kako od dane podgrupe $H \leq G, H \neq G$ konstruirati novu podgrupu M koja će sadržavati H i još barem jedan element a koji nije u H. Dobivenu grupu M označimo simbolom $\langle H; a \rangle$. Dakle,

$$\langle H; a \rangle = \{xa^k : x \in H, 0 \leq k < l\},$$

gdje je l indikator od a u H. Primjenimo ovu konstrukciju više puta, počevši od podgrupe $G_1 = \{e\}$. Ako je $G_1 \neq G$, neka je $a_1 \in G \backslash G_1$ pa definirajmo $G_2 = \langle G_1; a_1 \rangle$. Ako je $G_2 \neq G$, neka je $a_2 \in G \backslash G_2$ pa definirajmo $G_3 = \langle G_2; a_2 \rangle$. Dalje nastavljamo analogno te dobivamo konačan skup elemenata $a_1, a_2, \ldots, a_t$ i pripadajući skup podgrupa $G_1, G_2, \ldots, G_{t+1}$ takvih da je

$$G_{r+1} = \langle G_r; a_r \rangle$$

te

$$G_1 \subset G_2 \subset \cdots \subset G_{t+1} = G.$$

Znamo da postupak završava u konačnom broju koraka jer je grupa G konačna, a svaka podgrupa G_{r+1} sadrži više članova od prethodne podgrupe G_r. Teorem sada dokazujemo induktivno: za dobiveni lanac podgrupa pokazat ćemo da ako tvrdnja vrijedi za G_r, vrijedit će i za G_{r+1}.
Jasno je da G_1 ima samo jedan karakter i to funkciju koja je identički jednaka 1. Nadalje, pretpostavimo da je podgrupa G_r reda m te da ona ima točno m različitih karaktera. Sada promotrimo $G_{r+1} = \langle G_r; a_r \rangle$ i neka je h indikator od a_r u G_r. Drugim riječima, h je najmanji prirodan broj takav da je ${a_r}^h \in G_r$. Sada ćemo pokazati da postoji točno h različitih načina proširenja pojedinog karaktera od G_r za dobivanje karaktera od G_{r+1} te da je svaki karakter od G_{r+1} proširenje nekog karaktera od G_r. Ovo će povlačiti da G_{r+1} ima točno mh karaktera, a znamo da je upravo toliko njezin red.
Elementi u G_{r+1} su oblika

$$x{a_r}^k, \quad x \in G_r, \quad 0 \leq k < h.$$

Pretpostavimo da je proširenje karaktera f od G_r do karaktera od G_{r+1} stvarno moguće. Nazovimo to proširenje $\widetilde{f}$. Odredimo $\widetilde{f}(x{a_r}^k)$. Zbog multiplikativnosti je

$$\tilde{f}(x{a_r}^k) = \tilde{f}(x)\tilde{f}(a_r)^k.$$

No, kako je $x \in G_r$, vrijedi $\widetilde{f}(x) = f(x)$ pa jednakost prelazi u

$$\widetilde{f}(x{a_r}^k) = f(x)\widetilde{f}(a_r)^k.$$

Uočimo da je $\widetilde{f}(x{a_r}^k)$ potpuno određen s $\widetilde{f}(a_r)$. Koje su moguće vrijednosti za $\widetilde{f}(a_r)$? Označimo $c = {a_r}^h$. Kako je $c \in G_r$, znamo da je $\widetilde{f}(c) = f(c)$, a zbog multiplikativnosti od $\widetilde{f}$ je i $\widetilde{f}(c) = \widetilde{f}(a_r)^h$. Dakle,

$$\widetilde{f}(a_r)^h = f(c),$$

pa je $\widetilde{f}(a_r)$ jedan od h-tih korijena od $f(c)$. Zato izbora za $\widetilde{f}(a_r)$ ima najviše h. Iz prethodnih razmatranja naslućujemo kako definirati proširenje $\widetilde{f}$. Ako je f dani karakter od G_r, odaberimo jedan od h-tih korijena broja $f(c)$, gdje je $c = {a_r}^h$ i definirajmo $\widetilde{f}(a_r)$ jednako odabranom korijenu. Na ostatku podgrupe G_{r+1} definirajmo proširenje $\tilde{f}$ pomoću jednakosti

$$\widetilde{f}(x{a_r}^k) = f(x)\widetilde{f}(a_r)^k.$$

Svih h odabira za $\widetilde{f}(a_r)$ su različiti, pa imamo h različitih načina za dobivanje $\widetilde{f}(x{a_r}^k)$. Uvjerimo se sada da proširenje $\widetilde{f}$ ima svojstvo multiplikativnosti. Imamo:

$$\begin{aligned}\widetilde{f}(x{a_r}^k \cdot y{a_r}^j) &= \widetilde{f}(xy \cdot {a_r}^{k+j}) = f(xy)\widetilde{f}(a_r)^{k+j} \\ &= f(x)f(y)\widetilde{f}(a_r)^k\widetilde{f}(a_r)^j \\ &= \widetilde{f}(x{a_r}^k)\widetilde{f}(y{a_r}^j),\end{aligned}$$

pa je $\widetilde{f}$ karakter od G_{r+1}. Nikoja dva proširenja $\widetilde{f}$ i $\widetilde{g}$ ne mogu biti jednaka na G_{r+1} jer bi karakteri f i g čija su oni proširenja bili jednaki na G_r. Zato se svaki od m karaktera od G_r može na h različitih načina proširiti do karaktera od G_{r+1}. Štoviše, ako je ϕ bilo koji karakter od G_{r+1}, njegova restrikcija na G_r je karakter od G_r, pa ovakvim postupkom proširenja dobivamo sve karaktere od G_{r+1}.

1. Grupa karaktera

Neka je G konačna Abelova grupa reda n. Glavni karakter od G označimo s f_1. Preostale karaktere grupe G označimo s $f_2, f_3, \ldots, f_n$. Oni nisu glavni karakteri pa imaju svojstvo $f(a) \neq 1$ za neki $a \in G$.

Teorem 3.3. *Skup svih karaktera grupe G uz operaciju množenja definiranu s*

$$(f_i f_j)(a) = f_i(a)f_j(a), \quad \forall a \in G$$

čini Abelovu grupu reda n. Ovu grupu označavamo s $\widehat{G}$. Neutralni element u $\widehat{G}$ je glavni karakter f_1. Inverz pojedinog karaktera f_i je njemu recipročan karakter $1/f_i$.

Dokaz: Lako se provjeri da $\widehat{G}$ zadovoljava sva svojstva grupe, pa dokaz izostavljamo.

Napomena 3.1. *Za svaki karakter f vrijedi $|f(a)| = 1$. Zato je recipročna vrijednost $1/f(a)$ jednaka kompleksno-konjugiranoj vrijednosti $\overline{f(a)}$. Dakle, funkcija $\overline{f}$ definirana s $\overline{f}(a) = \overline{f(a)}$ je također karakter grupe G. Štoviše, vrijedi*

$$\overline{f}(a) = \frac{1}{f(a)} = f(a^{-1}), \quad \forall a \in G.$$

2. Relacije ortogonalnosti

Neka je G konačna Abelova grupa reda n s elementima $a_1, a_2, \dots, a_n$ te $f_1, f_2, \dots, f_n$ karakteri grupe G, gdje je f_1 glavni karakter.

Označimo s $A = A(G)$ $n \times n$ matricu $[a_{ij}]$ čiji je element u i-tom retku i j-tom stupcu jednak

$$a_{ij} = f_i(a_j).$$

Pokazat ćemo da je matrica A invertibilna, a taj će nas zaključak dovesti do relacija ortogonalnosti među karakterima. Za početak, odredimo sumu elemenata u pojedinom retku matrice A.

Teorem 3.4. *Suma elemenata u i-tom retku matrice A dana je s*

$$\sum_{r=1}^{n} f_i(a_r) = \begin{cases} n & \text{ako je } i = 1, \\ 0 & \text{inače.} \end{cases}$$

Dokaz: Označimo traženu sumu sa S. Ako je $f_i = f_1$, svaki pribrojnik u sumi je 1, pa je $S = n$. Ako je $f_i \neq f_1$, tada $\exists b \in G$ za koji je $f_i(b) \neq 1$. Uzmemo li sada za a_r redom elemente grupe G, dobivamo n različitih produkata ba_r. Dakle,

$$S = \sum_{r=1}^{n} f_i(ba_r) = f_i(b) \sum_{r=1}^{n} f_i(a_r) = f_i(b)S.$$

Odavde slijedi $S(1 - f_i(b)) = 0$. Kako je $f_i(b) \neq 1$, slijedi $S = 0$.

Pokažimo sada, kako smo ranije najavili, da je A invertibilna.

Teorem 3.5. *Neka A^* označava hermitski adjungiranu matricu matrici A. Vrijedi*

$$AA^* = nI,$$

gdje je I $n \times n$ jedinična matrica. Dakle, $A^{-1} = \frac{1}{n}A^*$.

Dokaz: Neka je $B = AA^*$. Element u i-tom retku i j-tom stupcu matrice B jednak je

$$b_{ij} = \sum_{r=1}^{n} f_i(a_r)\overline{f_j}(a_r) = \sum_{r=1}^{n} (f_i\overline{f_j})(a_r) = \sum_{r=1}^{n} f_k(a_r),$$

gdje je $f_k = f_i\overline{f_j} = f_i/f_j$. Znamo da je $f_i/f_j = 1$ ako i samo ako je $i = j$. Sada iz prethodnog teorema slijedi

$$b_{ij} = \begin{cases} n & \text{ako je } i = j, \\ 0 & \text{ako je } i \neq j. \end{cases}$$

Drugim riječima, $B = nI$.

Teorem 3.6. (Relacije ortogonalnosti među karakterima) *Vrijedi:*

$$\sum_{r=1}^{n} \overline{f_r}(a_i) f_r(a_j) = \begin{cases} n & \textit{ako je } a_i = a_j, \\ 0 & \textit{ako je } a_i \neq a_j. \end{cases}$$

Dokaz: Iskoristimo činjenicu da matrica komutira sa svojim inverzom. Imamo $AA^* = A^*A = nI$. Tvrdnja sada slijedi direktno jer je suma u teoremu jednaka upravo elementu u i-tom retku i j-tom stupcu matrice A^*A.

Napomena 3.2. *Kako je $\overline{f_r}(a_i) = f_r(a_i)^{-1} = f_r({a_i}^{-1})$, opći član sume u prethodnom teoremu jednak je $f_r({a_i}^{-1})f_r(a_j) = f_r({a_i}^{-1}a_j)$. Relacije ortogonalnosti stoga se mogu izraziti i na sljedeći način:*

$$\sum_{r=1}^{n} f_r({a_i}^{-1} a_j) = \begin{cases} n & \textit{ako je } a_i = a_j, \\ 0 & \textit{ako je } a_i \neq a_j. \end{cases}$$

Ako uzmemo $a_i = e$, dobivamo sljedeći rezultat:

Teorem 3.7. *Suma elemenata u j-tom stupcu matrice A dana je s*

$$f_r(a_j) = \begin{cases} n & \textit{ako je } a_j = e, \\ 0 & \textit{inače.} \end{cases}$$

Poglavlje 4

Dirichletovi karakteri

Do sada smo se bavili karakterima proizvoljne konačne Abelove grupe G. Neka je sada G reducirani sustav ostataka modulo fiksni prirodni broj k. Prije svega, naravno, pokazat ćemo da je uz prikladno definirano množenje G uistinu multiplikativna grupa.

Prisjetimo se, reducirani sustav ostataka modulo k je skup od $\varphi(k)$ prirodnih brojeva $\{a_1, a_2, \ldots, a_{\varphi(k)}\}$ međusobno nekongruentnih modulo k. Svi elementi ovog skupa su relativno prosti sa k. Za svaki cijeli broj a odgovarajući ostatak $\hat{a}$ je skup svih cijelih brojeva kongruentnih a modulo k:

$$\hat{a} = \{x : x \equiv a \pmod{k}\}.$$

Množenje ostataka definiramo s

$$\hat{a} \cdot \hat{b} = \widehat{ab}.$$

Dakle, produkt dvaju ostataka $\hat{a}$ i $\hat{b}$ je ostatak produkta ab.

Teorem 4.1. *Uz prethodno definirano množenje, reducirani sustav ostataka modulo k je konačna Abelova grupa reda $\varphi(k)$. Neutralni element ove grupe je ostatak $\hat{1}$. Inverz ostatka $\hat{a}$ je ostatak $\hat{b}$ takav da je $ab \equiv 1 \pmod{k}$.*

Dokaz: Svojstvo zatvorenosti zadovoljeno je samom definicijom množenja ostataka. Očito je da je $\hat{1}$ neutralni element. Ako vrijedi $(a, k) = 1$, tada $\exists! b$ takav da je $ab \equiv 1 \pmod{k}$. Dakle, inverz od $\hat{a}$ je $\hat{b}$. Napokon, jasno je da je grupa Abelova te da je njezin red $\varphi(k)$.

Definicija 4.1. (Dirichletovi karakteri) *Neka je grupa G reducirani sustav ostataka modulo k. Za karakter f grupe G definiramo aritmetičku funkciju* $\chi = \chi_f$ *na sljedeći način:*

$$\chi(n) = \begin{cases} f(\hat{n}) & \textit{ako je } (n,k) = 1, \\ 0 & \textit{ako je } (n,k) > 1. \end{cases}$$

Funkciju χ *nazivamo Dirichletov karakter modulo k. Glavni karakter* χ_1 *je onaj sa svojstvom*

$$\chi_1(n) = \begin{cases} 1 & \textit{ako je } (n,k) = 1, \\ 0 & \textit{ako je } (n,k) > 1. \end{cases}$$

Teorem 4.2. *Postoji točno* $\varphi(k)$ *različitih Dirichletovih karaktera modulo k te je svaki od njih multiplikativan i periodičan s periodom k. To jest, vrijedi*

$$\chi(mn) = \chi(m)\chi(n), \quad \forall m, n$$

i

$$\chi(n + k) = \chi(n), \quad \forall n.$$

Obratno, ako je χ *mlultiplikativna funkcija te periodična s periodom k te je za* $(n, k) > 1$ $\chi(n) = 0$*, tada je* χ *jedan od Dirichletovih karaktera modulo k.*

Dokaz: Kako postoji $\varphi(k)$ karaktera za grupu G koja je reducirani sustav ostataka modulo k, karaktera χ_f modulo k ima također $\varphi(k)$. Svojstvo multiplikativnosti χ_f se nasljeđuje od f kada su oba m i n relativno prosti s k. Ako jedan od njih nije relativno prost s k, tada nije ni mn, pa je $\chi(mn) = \chi(m)\chi(n) = 0$. Svojstvo periodičnosti slijedi iz činjenice da je $\chi_f(n) = f(\hat{n})$ te da $a \equiv b \pmod k$ implicira $(a, k) = (b, k)$. Što se tiče obrata, uočimo da je funkcija definirana na G izrazom

$$f(\hat{n}) = \chi(n), \quad \text{ako je} \quad (n, k) = 1$$

karakter grupe G, pa je χ Dirichletov karakter modulo k.

Primjer 4.1. *Za* $k = 1$ *ili* $k = 2$ *imamo* $\varphi(k) = 1$ *pa je jedini Dirichletov karakter glavni karakter* χ_1*. Za* $k \geq 3$ *slijedi* $\varphi(k) \geq 2$*, pa postoje barem dva Dirichletova karaktera. Iduće tablice prikazuju sve Dirichletove karaktere za* $k = 3, 4$ *i* 5*.*

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0

$k = 3,\ \varphi(k) = 2$

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	-1	0

$k = 4,\ \varphi(k) = 2$

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	$-i$	-1	0
$\chi_4(n)$	1	$-i$	i	-1	0

$k = 5,\ \varphi(k) = 4$

Pri popunjavanju ovih tablica koristimo činjenicu da vrijedi $\chi(n)^{\varphi(k)} = 1$ kad god je $(n, k) = 1$, pa je $\chi(n)$ $\varphi(k)$-ti korijen jedinice. Uočimo da vrijedi i sljedeće: ako je χ karakter modulo k, njegov kompleksno konjugirani karakter $\overline{\chi}$ je također karakter modulo k. Ove informacije su dovoljne za popunjavanje tablica za $k = 3$ i $k = 4$.

Za $k = 5$ imamo $\varphi(k) = 4$, pa su moguće vrijednosti za $\chi(n)$ ± 1 i $\pm i$ kada je $(n, 5) = 1$. Osim toga, $\chi(2)\chi(3) = \chi(6) = \chi(1) = 1$, pa su $\chi(2)$ i $\chi(3)$ međusobno inverzni. Kako je $\chi(4) = \chi(2)^2$, imamo sve potrebne informacije da bismo popunili tablicu za $k = 5$. Prisjetimo se, kao provjeru možemo koristiti i prethodno dokazane teoreme koji govore da je suma elemenata u svakom retku i stupcu osim u prvom jednaka 0.

Iduće dvije tablice prikazuju sve Dirichletove karaktere modulo 6 i 7.

n	1	2	3	4	5	6
$\chi_1(n)$	1	0	0	0	1	0
$\chi_2(n)$	1	0	0	0	-1	0

$k = 6,\ \varphi(k) = 2$

n	1	2	3	4	5	6	7
$\chi_1(n)$	1	1	1	1	1	1	0
$\chi_2(n)$	1	1	-1	1	-1	-1	0
$\chi_3(n)$	1	ω^2	ω	$-\omega$	$-\omega^2$	-1	0
$\chi_4(n)$	1	ω^2	$-\omega$	$-\omega$	ω^2	1	0
$\chi_5(n)$	1	$-\omega$	ω^2	ω^2	$-\omega$	1	0
$\chi_6(n)$	1	$-\omega$	$-\omega^2$	ω^2	ω	-1	0

$k = 7,\ \varphi(k) = 6,\ \omega = e^{\pi i/3}$

Iskažimo još i dokažimo idući teorem, koji govori o relacijama ortogonalnosti za karaktere modulo k.

Teorem 4.3. *Neka su $\chi_1, \ldots, \chi_{\varphi(k)}$ $\varphi(k)$ Dirichletovih karaktera modulo k te neka su $m, n \in \mathbb{N}$ takvi da je $(n, k) = 1$. Tada vrijedi:*

$$\sum_{r=1}^{\varphi(k)} \chi_r(m)\overline{\chi_r}(n) = \begin{cases} \varphi(k) & \text{ako je } m \equiv n \pmod{k}, \\ 0 & \text{ako je } m \not\equiv n \pmod{k}. \end{cases}$$

Dokaz: Ako je $(m, k) = 1$, dovoljno je uzeti $a_i = \hat{n}$ i $a_j = \hat{m}$ i iskoristiti relacije ortogonalnosti poznate otprije. Uočimo i da je $\hat{m} = \hat{n}$ ako i samo ako je $m \equiv n \pmod{k}$. Ako je $(m, k) > 1$, svi pribrojnici u sumi su jednaki 0 te je $m \not\equiv n \pmod{k}$.

Literatura

[1] Tom M. Apostol, *Introduction to Analytic Number Theory (Undergraduate Texts in Mathematics)*, Springer Science+Business Media New York, 2010.,129–140.